AFFIDAVIT

I, Michael McCullagh, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS), a department in the executive branch of the United States of America. ICE is the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since July 2002. Upon graduating from the Federal Law Enforcement Training Center, I was assigned as a Special Agent for the U.S. Customs Service in the Special Agent in Charge (SAC) New York Office in New York City. In October 2007, I transferred to the Burlington, Vermont Resident Agent in Charge Office, where I presently work. I hold a Bachelor of Science degree in Business Administration from Saint Michael's College. I have been a computer forensic agent (CFA) for my agency since 2006 and have participated in many child pornography and child exploitation investigations. Prior to my employment with HSI, I was a police officer with the Winooski, Vermont Police Department.

2. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

PURPOSE OF WARRANT

3. I make this Affidavit in support of a finding of probable cause to issue a warrant, pursuant to Fed. R. Crim. P. 41(b)(1), (e)(2)(A), and (e)(2)(B), to seize and search electronically

stored information on the Target Media, defined as digital devices and media accessing the Internet through Waitsfield and Champlain Valley Telecom account 200155513, assigned to username "sremick," name - Scott Remick, and physical address 1153 Hardscrabble Road, Bristol, Vermont, further described in Attachment A, which is attached hereto and incorporated herein. The Waitsfield and Champlain Valley Telecom account 200155513 referenced above is referred to herein as the Account. In particular, I request approval to access the Target Media remotely to exfiltrate, or seize, the electronically stored information contained thereon, and to copy such stored information onto electronic storage media controlled by law enforcement.[1]

4. I make this affidavit in support of a warrant to search the Target Media for evidence and instrumentalities of the following statutes: knowing possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(b), knowing transportation of child pornography, in violation of 18 U.S.C. § 2252(a)(1), and knowing receipt and distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) (collectively referred to as the Subject Offenses). The evidence and instrumentalities to be seized and searched are described in Attachment B, which is attached hereto and incorporated herein.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. The information contained in this affidavit is based upon my training, experience, investigation, and consultation with other members of law enforcement. Because this affidavit is being submitted for the limited purpose of securing a warrant to search the Target Media, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts which I believe

[1] The use of remote access to search electronic storage media and to seize or copy electronically stored information is permissible. *See, e.g.*, Fed.R.Crim.P. Rule 41(b)(6) (addresses venue issues for remote access of digital media and electronically stored information); *United States v. Eldred*, 933 F.3d 110 (2d Cir. 2019) (venue challenge to Magistrate Judge's issuance of remote access search technique, not to use of remote access technique).

are necessary to establish probable cause to believe evidence and instrumentalities of the crimes described above are located on the Target Media. Where I have reported statements by others or from documents that I have reviewed, those statements are reported in substance and in part, unless otherwise indicated.

TECHNICAL TERMS AND BACKGROUND

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **IP Address**: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses. There are two commonly used types of IP addresses called IPv4 and IPv6. IPv4, or IP version 4, is a 32-bit numeric address that consists of a series of four numbers, each ranging between 0 and 255, that are separated by dots. An example of an IPv4 address is 123.111.123.111. IPv6, or IP version 6, is a 128-bit hexadecimal address that consists of a series of eight values separated by colons. Hexadecimal values consist of a series of numbers between 0 and 9 and letters between A and F. An example of an IPv6 address is: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

b. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. **Storage medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. **"Child Pornography"** includes any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

e. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

f. **"Sexually explicit conduct"** applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

g. **"Visual depictions"** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

h. **Dark Web:** The clear, surface, or open web is part of the Internet accessible to anyone with a standard internet browser and one that standard web search engines can index. The deep web is the part of the internet whose contents are not indexed by standard web search engines. The dark net or dark web is a part of the deep web that not only cannot be discovered through a traditional search engine, but also has been intentionally hidden and is inaccessible through standard browsers and methods. The dark web is accessible only with specific software, configurations, and/or authorization, including non-standard communications protocols and ports, such as a TOR ("The Onion Router") browser. A TOR browser is designed specifically to facilitate anonymous communication over the internet. In order to access the TOR network, a user must install TOR software either by downloading an add-on to the user's web browser or by downloading the free "TOR browser bundle." Use of the TOR network bounces a user's encrypted communications through a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user. Because of the way TOR routes communications through other computers, traditional IP identification techniques are not viable. When a user on the TOR network accesses a website, for example, the IP address of a TOR "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that TOR exit node IP address. A criminal suspect's use of TOR makes it extremely difficult for law enforcement agents to detect a host, administrator, or user actual IP address or physical location.

i. **Operating System.** An operating system is software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals. Examples of common operating systems currently in use include Microsoft Windows, macOS, Linux, and mobile operating systems, such as iOS (iPhones/iPads) or Android.

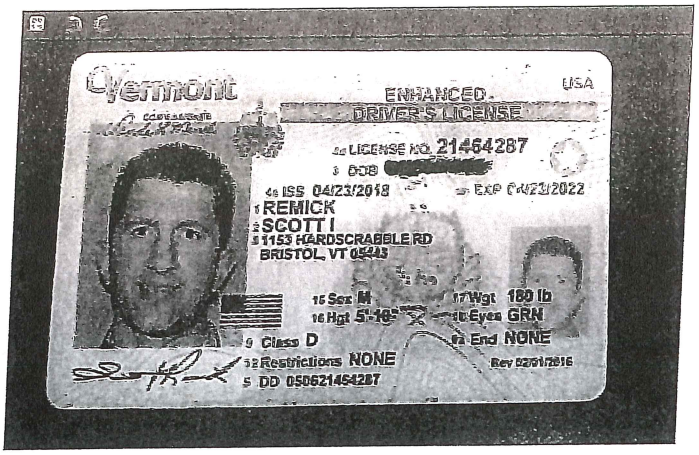
j. **Communication Port Number.** A communication port number is information that helps computers associate a communication with a particular program or software process running on that computer. For example, if a communication is sent to port 80, a receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

k. **Web Browser Header Information.** Web browser header information is public-facing information provided by computers via their browser to internet websites. This header information includes for instance the language on the computer, the "USER-AGENT," which includes the browser type, operating system, and browser version, and other information that can help websites serve dynamic content depending on the specific software, operating systems, screen resolutions, and other dynamic variables on a computer. This information also includes information regarding the web browser and other client software installed on the computer, including but not limited to Microsoft Office and Adobe Reader, including the user agent strings associated with the software, which may include the version of the software running on the computer.

PROBABLE CAUSE

7. On the evening of June 16, 2021, a source of information (SOI) contacted the Vermont State Police (VSP) to report that it believed that an individual residing in Bristol, Vermont, was in possession of child pornography. The SOI also sent an email to VSP which detailed its findings. On June 17, 2021, VSP contacted HSI SA Alex Zuchman, assigned to HSI Burlington, regarding this information and provided to SA Zuchman contact information for the SOI. VSP also forwarded the email sent by the SOI. I have reviewed this email message. It is reproduced, in pertinent part, below:

> I am security research [sic] who came upon this individual. A program I wrote scans the internet for misconfigured computers. This week a bot was able to enter his computer through an unsecured hole in his network. The hole allowed the bot to view, what looks like a great deal of child porn. I am not sure how to handle this and I am attempting to do the moral thing here. The following files are present on his system which let me identify him.
>
> His ID: This picture was present on his desktop.



His IP:
"ip": "209.99.193.74",
"hostname": "pppoe-209-99-193-74.greenmountainaccess.net",
"city": "Charlotte",
"region": "Vermont",
"country": "US",
"loc": "44.3098,-73.2610",
"org": "AS12282 Selectronics Corp.",
"postal": "05445",
"timezone": "America/New_York",
"readme": "https://ipinfo.io/missingauth"

The Content: So far I have only had the stomach to open 7 images and they were all child porn. I have attached a listing of all the files I have seen in one part of his encrypted drive. His network contains TB's of content on various encrypted devices. Unplugging them or detaching them will result in the drives locking and all the content becoming unavailable. I suspect you will need some cooperation with him to gain full access to all these files if they are indeed secured correctly. He also is running a variety of services on TOR which I assume he is using to receive and transmit this data. From my perspective, I can only imagine what these devices are for and I frankly don't want to know.

This is the evidence I have. I apologize if this is not enough, I again am just attempting to do the right thing here. What I saw shook me to my core and I honestly could have never imagined being here in this position. This is fairly routine and innocuous research I do with a private team that analyzes the impact of security breaches.

8. The SOI's email had an attachment: a text file named "files.txt" (the Text File). I have reviewed the Text File and observed the following:

a. It contained a list of directories from the Target Media, as well as the names of the files contained within these directories. I do not know if this is a complete listing of the files. Based on my communications with the SOI, I do not believe that it is.

b. The Text File does not contain any actual content from the Target Media. Many of the filenames I saw indicated that the files likely contained child exploitation material. Examples of the filenames are: "(XXXX) German Girl 14 Years Masturbation On Webcam.avi," "10Yo Girl Spreads And Plays With Hairless Pussy For Webcam - 2004.avi," "Julia 7yo – First Assfuck.avi.avi,." and "10Yo Nadian REALLY CUMS!!! Masturbates Very Pink Pussy On Webcam!.avi." I also observed that many filenames contained phrases that I know, based on my training and experience, are used to identify child exploitation material. I have not reproduced these phrases here to keep them out of the public domain if this search warrant is ever unsealed.

9. On June 17, 2021, SA Zuchman and I spoke with the SOI over the phone. In this conversation, the SOI disclosed the following[2]:

a. He/she is a private software developer and security analyst. The SOI is part of a small group of individuals involved in analyzing a very specific piece of software with a specific security vulnerability. As part of this work, this group has developed a software "bot" to search for computers/servers using this specific piece of software, which still have this known

---

[2] Through additional conversations with the SOI, HSI has learned the following about the SOI: The SOI has no criminal history. The SOI has mental health issues which require it to take medication. The medication does not affect the SOI's mental faculties or recall; the medication addresses mood and depression issues.

The SOI voluntarily made the initial disclosures to law enforcement about what it discovered without any agreement with the government. Beginning on June 23, 2021, the SOI's communications with the government were made pursuant to a "proffer letter" agreement. On June 28, 2021, the SOI and the government entered into a letter immunity agreement, which granted immunity co-extensive with 18 U.S.C. § 6001, *et seq.*, for disclosures made by the SOI pursuant to the agreement.

security issue. The bot identified a computer (part of the Target Media) with this security flaw (Computer 1).[3]

1. Based on my training and experience, I know that the term "bot," is short for robot. It refers to a software program which performs automated, repetitive, pre-defined tasks.

b. The SOI looked at the profile of the computer (Target Media) and noticed it was running a Linux Operating System, as well as using LUKS. The SOI also noticed a VeraCrypt volume mounted on the Target Media named "VeraCrypt 1".

1. Based on my training and experience, I know the following: (1) LUKS is an acronym for Linux Unified Key Setup, which is a full disk encryption intended for the Linux Operating System; (2) VeraCrypt is a freeware utility used for on-the-fly encryption. A VeraCrypt volume is, simply put, a container that has a potentially unbreakable level of encryption. VeraCrypt allows a user the ability to create a virtual encrypted disk within a file or encrypt a partition. Once created on a computer, a VeraCrypt volume can be moved to different locations on the computer, or stored on external media like removable hard drives and USB storage devices; and (3) a "mounted" drive exists where the operating system has made the files/directories on storage media available for users to access through the file system.

c. The SOI also observed the presence of a TOR (The Onion Router) browser on the Target Media. The SOI also observed other folders labeled "VeraCrypt 2" and "VeraCrypt 3 also on the Target Media.

[3] Computer 1 is discussed further in paragraph 10.

1. Based on my training and experience, I know that the TOR browser has many uses, both legal and illegal. I do know that it is commonly used by persons who are interested in child pornography because the user's identity is, generally, obscured.

d. The SOI looked at the contents of the VeraCrypt 1 volume and viewed some of the image files within this volume. The SOI saw approximately five or six images, maybe seven, of what the SOI identified as child pornography. The SOI then stopped looking at image files. The SOI indicated there were many additional images in the VeraCrypt 1 volume.

e. The SOI also observed the Thunderbird email client installed on the Target Media. The SOI recalled there were many email messages within this client. The SOI also recalled a folder named "to jenny," or something to that effect. The SOI looked in this folder and observed that it was also full of what the SOI believed was child pornography.

1. I looked for a folder named "Jenny" or "Jennie" in the Text File but did not locate a folder with this name. I found many files with the name "Jenny" in the file name in the Text File. I located numerous instances of "Jeanie" as a directory name, including but not limited to directories named "For Jeanie/Pearl Lolitas," and "For Jeanie/Videos."

a. Based on my training and experience, I know that the term "Lolita" can refer to child pornography.

f. The SOI located an image of a Vermont Enhanced Driver's License, which was saved on the Target Media. The SOI provided this license in its email to the VSP.

g. The SOI looked through the Target Media on or about June 16, 2021 at approximately 8:00 PM Eastern Time.

10. On June 30, 2021, Elijah Brigham, an HSI Cyber Operations Officer, and I spoke with the SOI specifically about how it discovered the child pornography on the Target Media. During this conversation, the SOI disclosed the following:

a. The security vulnerability that he and his colleagues are researching (see paragraph 9(a), *supra*) identified a computer with an IP address that resolved to Germany. The user of this computer was "Scott."

1. For purposes of this section, I will refer to this computer as "Computer 1," though Computer 1 is also part of the collective Target Media for the purposes of this affidavit.

b. Based on the internal network configuration/information of Computer 1, the SOI suspected that Computer 1 was not at the same location as the IP address in Germany.

c. The SOI was able to identify another computer (Computer 2) on the same local network as Computer 1. The SOI asked Computer 2 to report its public IP address. Computer 2 provided IP address, 209.99.193.74, which resolves to an ISP in Vermont.

1. The SOI provided the following analogy to explain the concept of what it did to identify the IP address for Computer 2: A computer on a home network using a Virtual Private Network (VPN) can make itself appear to be elsewhere. A second device on that same network, if not also using a VPN, is most likely, if accessed and queried as to the IP address it is using, to return an accurate public IP address. It will thus provide the actual physical location of the device.

d. Based on the SOI's experience as a security researcher, and the below facts, the SOI believes that IP address 209.99.193.74 is the accurate location for the Target Media:

1. The user of Computer 1 was "Scott."

2. Another computer in the same internal network as Computer 1 provided its IP address as 209.99.193.74.

3. The SOI located an image of a Vermont Enhanced Driver's License, issued to Scott I. Remick, of Bristol, Vermont, saved on the Target Media.

11. A search of publicly available records located online determined that IP address 209.99.193.74 was assigned to a company known as Waitsfield and Champlain Valley Telecom. I caused a Department of Homeland Security summons to be served on Waitsfield and Champlain Valley Telecom for subscriber information for IP address 209.99.193.74 on June 16, 2021 at 8:00 PM EST. This request also included 180 days of IP address history. On June 22, 2021, a representative from Waitsfield and Champlain Valley Telecom responded and provided the following information regarding the Account:

a. "The IP address on the date in question was assigned to user 'sremick.' That IP has been assigned to that customer since 4/18/2021 and is still assigned."

b. The username "sremick" is assigned to:

Account#:	200155513
Name:	Scott Remick
Address:	1153 Hardscrabble Road Bristol, VT 05443
Phone:	802-453-3698

c. "Customer has phone and broadband service since 2014. Customer pays with recurring credit card ending 4877. We do not store additional credit card information for security purposes. Customer does not have email with GMA (Green Mountain Access), but the customer has provided email scott@sremick.net for correspondence purposes."

d. The company also provided six months of IP History and also noted that "Green Mountain Access (GMA) dynamically assigns IP's, so each modem reboot can result in a new IP assignment."

12. I caused a search to be done of the Vermont Department of Motor Vehicles (DMV) databases for information regarding Vermont Driver's License Number 21464287. I learned that license number was issued to Scott I. Remick, 1153 Hardscrabble Road, Bristol, VT 05443. Additional record checks conducted with Vermont DMV show that Scott Remick (born in 1975) and Gina Wrest (born in 1988) have active Vermont driver's licenses and provided 1153 Hardscrabble Road, Bristol, VT as their residential address. Scott Remick has a 2014 Subaru Impreza, bearing Vermont registration SCOOTER, registered to him. Gina Wrest has a 2017 Toyota RAV4, bearing Vermont registration GKW286, registered to her.

13. I conducted an open-source search on publicly available websites and determined that Scott I. Remick is a Senior Technology Specialist for Middlebury College in Middlebury, Vermont. I also located a website associated with Remick named "vtgeek.com." The opening page of the website provided the following information about Remick:

> My name is Scott Remick and I am a Vermont native who has been living in the Addison County area all my life. Since entering the workforce, every job I've had has been with computers and the IT field, including working for a small local computer store that grew to eight times the size after I started, to repairs and IT administration for local companies. I now have 30 years of computer and technology experience under my belt, covering all aspects of software and hardware. I am certified by Apple, Dell, Microsoft, and CompTIA. I am employed by a large institution in the IT department during regular business hours, but I am available nights and weekends to offer my services to you. With all my work over the years being in the Middlebury and surrounding areas, I have built up a loyal clientele and plenty of references available to new clients. With an unmatched skill set, decades of experience, and rates below the competition, make me your first choice when you need computer assistance!

14. The contact information on this webpage provided a phone number, (802) 453-3698. This is the same number associated with the subscriber information provided by Waitsfield and Champlain Valley Telecom.

15. On June 22, 2021 at approximately 9:00 am, SA Zuchman traveled to 1153 Hardscrabble Road, Bristol Vermont. He observed two vehicles parked in the driveway of this residence, a Subaru, black in color, and a Toyota RAV4, blue in color. SA Zuchman was able to observe that both of the vehicles displayed Vermont registration plates but was unable to obtain their specific registration numbers from his location. These vehicles match the vehicles registered to Scott Remick and Gina Wrest.

16. On June 22, 2021, I was contacted by Detective Matthew Raymond from the Vermont Attorney General's Office, who is also the Commander of the Vermont Internet Crimes Against Children (ICAC) Task Force. Det. Raymond told me that he had recently received a CyberTipline Report (#93128658) from the National Center for Missing and Exploited Children (NCMEC) regarding a recent report to NCMEC from a member of the public. The reporting person did not provide a name but NCMEC logged the caller's number, which I recognized as being the one used by the SOI. (I have confirmed with the SOI that it made this report to NCMEC.) The report to NCMEC occurred on June 17, 2021 at 01:01:55 UTC (Universal Time Coordinated). When the captured report time is converted to Eastern Daylight Time (EDT), the report time would be June 16, 2021 at approximately 9:01 pm. The SOI had reported that it had accessed the Target Media on June 16, 2021 at approximately 8:00 pm, Eastern Time.

17. I have reviewed the NCMEC report, which contained the following:

> A member of the public submitted this report concerning allegations of child pornography. The reporting person claims the suspect is chatting with and exchanging child pornography with the chat participant on the Tor network. The reporting person

alleges the suspect has large amounts of child pornography on an encrypted drive, which the reporting person claims appeared to be unencrypted at the time this report was made on 6/17/2021. The reporting person claims the chat participant and the suspect may possibly be in a sexual relationship. The reporting person is concerned the chat participant may possibly be a minor. CT/TA queries yielded negative or irrelevant results. This report has been made available to the VT ICAC concerning the suspect based on reported IP and TLO results. This report has also been made available to the VT ICAC concerning the chat participant based on possible related TLO results.

The caller reported that the reported person has access to and is distributing child pornography. He is communicating with Jeanie. It is believed that she may be a teenager. The reported person and Jeanie are either trading images or having a relationship. The child pornography is on the reported persons computer and hard drive. The caller stated that the reported person will attempt to delete the images upon the arrival of law enforcement. He stated that the information is time sensitive. The caller was advised that if immediate assistance is needed he would need to contact law enforcement.

Reported Person
Scott Remick
04/23/1975
1153 Hard Scraple [sic] Road, Bristol, Vermont 05443
Facebook: www.facebook.com/siremick
Tor (server that the reported person is using to distribute child pornography)
IP: 2099919374
Employment: IT Technician

Jeanie
jeanie.elle@gmail.com"

I listened to the call recording and saved a copy to this report. The following additional information was provided by the reporting person:
On 6/17/2021, the reporting person claims the suspects data was on encrypted drives that were unencrypted at the time this report was made; reporting person is concerned that the suspect will encrypt the data or unplug the drives upon the arrival of law enforcement and data may become unable to retrieve. The reporting person believes the suspect may also become aware that the reporting person was able to access their drives and may have done the same once becoming aware.
The correct spelling of the reported identifiers are listed below:

1153 Hardscrabble Road, Bristol, VT 05443
IP: 209.99.193.74"

18. On June 23, 2021, SA Zuchman and I, among others involved in this investigation, spoke with the SOI over a video call. During this conversation, the SOI provided a description of several of the child pornography and child exploitation images from memory; the SOI did not save any of the image files it viewed. A description of some of the files are below. The SOI did not recall the filenames for these image files, so I am referencing them as first, second, third, for purposes of this affidavit:

a. First Image: A female child, approximately 10-14 years old, in a "69" position with a much older adult male. The male and this child were involved in a sex act together.

1. I understood the SOI's reference to a "69" sex act to mean that both individuals are performing oral sex on each other at the same time.

b. Second Image: A female child, approximately 12-13 years old, fully nude with her legs spread wide open. No pubic hair or breast development was observed.

c. Third Image: A possibly European teen, maybe Scandinavian, approximately 15-16 years old, topless with her breasts exposed.

19. During this video call, the SOI also advised it had installed two separate methods to access the Target Media at a later time, to which it referred as a "backdoor." The SOI installed the backdoors so law enforcement could access the Target Media remotely and without the user of the Target Media's knowledge in case the vulnerability that allowed it to access the Target Media no longer existed. The SOI also included a protocol in the backdoor whereby it regularly communicated from the Target Media to the SOI's computer (the Ping). The Ping was established to keep the backdoor open and viable. The Ping does not access content from, or

communicate with, the Target Media; its sole function is to keep the communication line to the backdoor open.

a. Based on my training and experience, I know that a "backdoor" is a typically covert method of bypassing normal authentication or encryption in a computer, as well as other devices. Backdoors are most often used for securing remote access to a computer, allowing access to privileged information such as passwords or data on hard drives.

20. On June 28, 2021, I caused a check to be conducted by the U.S. Postal Service to determine who was currently receiving mail at 1153 Hardscrabble Road in Bristol, Vermont. The response to this request indicated that Scott Remick and Gina Wrest receive mail at that address.

21. Based on the foregoing, I am seeking a warrant to search the Target Media (described in attachment A) for information (described in Attachment B) by remote means (described further below).

CHARACTERISTICS OF CHILD PORNOGRAPHERS

22. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to many individuals involved in such crimes:

a. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion

pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, or in some other secure location.

d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area.

e. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes, also may correspond with others to share information and materials.

THE REMOTE SEARCH TECHNIQUE

23. Based on my training and experience, and the communications I have had with the SOI, HSI personnel, and other law enforcement partners/resources, I have concluded that using a remote search technique is necessary to gain access to information that may otherwise be unavailable because of the subject user's efforts to conceal his activities. Specifically, the SOI detailed the encryption present on the Target Media, and mentioned that "[u]nplugging them or detaching them will result in the drives locking and all the content becoming unavailable." (*See* paragraph 7, *supra*). Accordingly, I request authority to use the remote search technique to investigate the Target Media.

24. The remote search of the Target Media will entail law enforcement remotely communicating with the Target Media in order to conduct an exfiltration of the information outlined in Attachment B to a government-controlled infrastructure, meaning government-

controlled storage media. Law enforcement will not make any changes to the Target Media beyond any changes to metadata that will occur as a result of accessing data during the search.

DELAYED NOTICE AND AFTER-HOURS EXECUTION

25. Pursuant to Fed. R. Crim. P. 41(f)(3), and 18 U.S.C. §3103a, I request permission to delay service of the warrant for up to 30 days after execution of the warrant because there is reasonable cause to believe that providing immediate notice of the warrant may have an adverse result, as defined by 18 U.S.C. § 2705. This is an ongoing investigation that is expected to continue after execution of this search warrant. If immediate notice of the warrant were to be served on the user of Target Media, it could result in flight from prosecution, destruction of evidence, or otherwise seriously jeopardize the ongoing investigation. Therefore, I request permission to delay service of the warrant until up to 30 days after execution of the warrant.

26. As outlined in this affidavit, the Target Media have a high degree of security associated with them, to include full disk encryption of the computer, as well as numerous VeraCrypt volumes which are also encrypted. Information obtained about Scott Remick, the suspected user, revealed he has over 30 years of computer experience and a sophisticated skill set. It appears he is currently employed as a Senior Technology Specialist at a local college. In light of the user's technical proficiency, I believe that it is possible that when law enforcement attempts to execute the search, it may not be able to gain access to the Target Media until after 10:00 pm. Accordingly, I request that this search warrant be allowed to be executed at any time in the day or night.

27. Therefore, I respectfully request that law enforcement is given the authority to remotely access the Target Media, and search/seize any of the items described in Attachment B

by transferring the contents thereof onto a law enforcement-controlled computer or storage device.

CONCLUSION

28. Based on the foregoing, I submit there is probable cause to search the Target Media, more specifically described in Attachment A, for the evidence and information outlined in Attachment B.

Dated at Burlington, in the District of Vermont, this 2nd day of July, 2021.

Michael McCullagh
Special Agent, HSI

Sworn to and subscribed before me this 2nd day of July, 2021.

Hon. Kevin J. Doyle
United States Magistrate Judge